The product of like-indexed terms in binary recurrences (Diophantine Problems and Analytic Number Theory)

AUTHOR(S):

Luca, F.; Walsh, P.G.

CITATION:

Luca, F. ...[et al]. The product of like-indexed terms in binary recurrences (Diophantine Problems and Analytic Number Theory). 数理解析研究所講究録 2003, 1319: 168-173

ISSUE DATE:

2003-05

URL:

http://hdl.handle.net/2433/43063

数理解析研究所講究録 1319 巻 2003 年 168-173

The product of like-indexed terms in binary recurrences

F. Luca and P.G. Walsh

November 1, 2002

Abstract

In recent work by Hajdu and Szalay, Diophantine equations of the form $(a^k-1)(b^k-1)=x^2$ were completely solved for a few pairs (a,b). In this paper, a general finiteness theorem for equations of the form $u_kv_k=x^n$ is described, where u_k and v_k are terms in certain types of binary recurrence sequences. Also, a unified computational approach for solving equations of the type $(a^k-1)(b^k-1)=x^2$ is described, and this approach was used to completely solve such equations for almost all (a,b) in the range $1<a<b\leq 100$. In the final section of this paper, it is shown that the *abc* conjecture implies much stronger results on these types of Diophantine problems. The interested reader can see more details in the full paper [9].

2000 Mathematics Subject Classification: 11D41,11B39

1 Introduction

There is a wealth of literature pertaining to the study of the arithmetical properties of terms in binary linear recurrences. In this paper, we attempt to consider the question of comparative results among pairs of such sequences. This type of question was raised in recent work of Szalay [19], and Hajdu and Szalay [8], wherein Diophantine equations such as

$$(a^k-1)(b^k-1)=x^2,$$

for fixed integers (a,b), were completely solved. In particular, all solutions (k,x) were determined for the particular values $(a,b)\in\{(2,3),(2,5),(2,6)\}$. Although the methods in these papers are relatively elementary, the results lead one to believe that there is a general theory lurking, as the arithmetic nature of terms in distinct sequences seem to behave in somewhat of an independent manner.

It is the purpose of this paper to describe a general finiteness theorem along these lines, and also to exhibit specific procedures for solving equations exactly of the type described above. Moreover, we hope to raise several outstanding questions in such a way as to motivate further research on these problems.

The paper is divided into three parts. In the first part of this paper, we describe a general finiteness theorem for the product of like-indexed terms in two binary recurrences to be a power of an integer. In the second part of the paper, we describe a method to completely solve Diophantine equations of the

form $(a^k-1)(b^k-1)=x^2$. We conclude with some discussion on open problems, and connections of this topic to the *abc* conjecture.

Throughout this paper, we use C_1, C_2, ... to denote effectively computable positive constants, which are either absolute, or depend only on some given parameters which will be specified.

2 A Finiteness Theorem

Let $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ denote non-zero integers. Define two sequences $\{u_k\}$ and $\{v_k\}$ by

$$u_k = c_1 a_1^k + d_1 b_1^k, \quad v_k = c_2 a_2^k + d_2 b_2^k.$$

To avoid degenerate cases, we assume that $|a_i| > |b_i|$ for $i = 1$ and 2.

Theorem 2.1 *Let e be a non-zero integer and let a_i, b_i, c_i, d_i denote non-zero integers for $i = 1, 2$. We assume that $|a_i| > |b_i|$ holds for $i = 1, 2$. Then, the equation*

$$u_k v_k = e x^n \tag{2.1}$$

with k, x and n integers, $k \geq 0$, $|x| > 1$, and $n > 1$ implies $n < C_1$, where C_1 is an effectively computable constant depending only on a_i, b_i, c_i, d_i, and e. Moreover, for any n fixed in the interval $3 \leq n < C_1$, equation (2.1) has only finitely many integer solutions (k, x) with $k \geq 0$. When $n = 2$, then equation (2.1) has also only finitely many integer solutions (k, x) with $k \geq 0$, except in one of the following two cases:

1. *$a_2 b_1 = a_1 b_2$ and $c_2 d_1 = c_1 d_2$.*
2. *$a_2 b_1 = -a_1 b_2$ and $c_2 d_1 = \pm c_1 d_2$.*

An immediate consequence of Theorem 2.1 is the following special case, which provided the motivation for much of this work.

Corollary 2.1 *Let $a > 1$ and $b > 1$ denote distinct integers. Then the equation*

$$(a^k - 1)(b^k - 1) = x^n$$

has finitely many solutions in integers (k, x, n) with $n > 1$.

The proof of Theorem 2.1 uses an effective result of Shorey and Stewart [18] together with an ineffective result of Corvaja and Zannier [5] concerning polynomial values in linearly recurrence sequences with positive integer roots. We remark that the ineffective result is based on the subspace theorem, thereby rendering our result ineffective. We begin by recalling the notation and the result from [5] which is relevant for our purposes.

Let $\mathcal{A}$ be the set of all functions $f : \mathbf{N} \to \mathbf{Q}$ such that either $f = 0$ identically, or there exist $r \geq 1$ distinct positive integers $\alpha_1 > \alpha_2 \ldots > \alpha_r > 0$, and non-zero rational numbers $\beta_1, \beta_2, \ldots, \beta_r$, such that

$$f(n) = \sum_{i=1}^{r} \beta_i \alpha_i^n, \tag{2.2}$$

for all positive integers n. For a given non-zero $f \in \mathcal{A}$ of the form (2.2), r is the *rank* of f, and we denote it by rank(f). The integers α_i $(i = 1, 2, \ldots, r)$ are the *roots* of f. The rational numbers β_i $(i = 1, 2, \ldots, r)$ are the *coefficients* of f.

For a non-zero $f \in \mathcal{A}$ its rank, roots and coefficients are uniquely determined. Also, $\mathcal{A}$ is a subring of the ring of all the rational valued functions defined on $\mathbf{N}$. $\mathcal{A}$ consists of all sequences of rational numbers which satisfy some linear recurrence with integer coefficients, and whose characteristic polynomial has distinct roots which are positive integers. The proof of Theorem 2.1 makes use of the following result from [5] (Corollary 1, page 320).

Lemma 2.1 *Let f be a non-zero element in $\mathcal{A}$ and let $n \geq 2$ be a fixed integer. If there exists a rational number e such that the diophantine equation*

$$f(k) = ex^n$$

has infinitely many integer solutions (k, x) with $k \geq 0$, then there exists $j \in \{0, 1, \ldots, n-1\}$, and an element $h \in \mathcal{A}$, such that if one denotes by g the element of $\mathcal{A}$ given by

$$g(k) := f(kn + j), \quad (k \in \mathbf{N}) \tag{2.2}$$

then $g = eh^n$.

Remark. Recently, Fuchs and Tichy [7] proved that if $n \geq 2$ and $e \neq 0$ are fixed integers, and $f \in \mathcal{A}$, $f \neq 0$, are such that the diophantine equation

$$f(k) = ex^n$$

has only finitely many integer solutions (k, x) with $k \geq 0$, then the number of such solutions is bounded by an effectively computable constant C_2 which depends only of n, e and f. Combining this result with our Theorem 2.1, it follows that the number of integer solutions (k, x, n) with $n \geq 3$ of equation (2.1) is bounded by an effectively computable constant C_2 depending only on a_i, b_i, c_i, d_i for $i = 1, 2$, and e, and that even the number of integer solutions (k, x) of equation (2.1) with $k \geq 0$ and $n = 2$ is also bounded by an effectively computable constant C_3 (depending, again, on a_i, b_i, c_i, d_i for $i = 1, 2$, and e) unless a_i, b_i, c_i, d_i satisfy one of the conditions 1 or 2 from the statement of the Theorem 2.1, and e is determined in terms of a_i, b_i, c_i, d_i (and can take at least one and at most two values) in which case equation (2.1) does have infinitely many integer solutions (k, x) with $k \geq 0$.

3 Computing all solutions of $(a^k - 1)(b^k - 1) = x^2$

Although for fixed $n \geq 2$, the result of the previous section is ineffective, being based on the ineffective result of Corvaja and Zannier, there are subclasses of those sequences in Theorem 2.1 for which all solutions can be determined for the particular case $n = 2$. In particular, for a fixed pair of positive integers (a, b), and under certain mild hypotheses, it was demonstrated in [9] how one can determine all integer solutions (k, x) with $k \geq 0$ to the Diophantine equation

$$(a^k - 1)(b^k - 1) = x^2.$$

We demonstrated our method by computing all solutions for almost all pairs (a, b) satisfying $2 \leq b < a \leq 100$. Difficulty arose primarily in the case that $(a - 1)(b - 1)$ is a square.

Theorem 3.1 *Let $2 \leq b < a \leq 100$ be integers, and assume that (a,b) is not in one of the following three sets:*
1. $\{(22,2),(22,4)\}$;
2. $\{\ (a,b)\ ;\ (a-1)(b-1)$ is a square, $a \equiv b \pmod 2$, and $(a,b) \neq (9,3),(64,8)\}$.
3. $\{\ (a,b)\ ;\ (a-1)(b-1)$ is a square, $a+b \equiv 1 \pmod 2$, and $ab \equiv 0 \pmod 4\}$.

If

$$(a^k-1)(b^k-1) = x^2, \tag{3.1}$$

then $k=2$, except only for the pair $(a,b)=(4,2)$, in which case the only solution to (3.1) occurs at $k=3$.

Of the 4851 pairs (a,b) satisfying $2 \leq b < a \leq 100$, Theorem 3.1 is able to deal with all but 70 of them. This is an improvement upon previous work of Szalay [19], wherein the particular case $(a,b)=(3,2)$ was solved, and on work by Hajdu and Szalay [8], wherein the case $(a,b)=(6,2)$ was solved.

The proof of Theorem 3.1 is accomplished in stages. Some general solvability results rule out many of the 4781 pairs that are solved. For the remaining pairs, a computational sieving method rules out the possibility of solutions for odd values of k. The proof is completed by using a result of Cohn [3], a deep theorem of Darmon and Merel [6], and properties of solutions to Pell equations (see [11]) to rule out solutions for even values of k.

4 Connections with the ABC conjecture

It is certainly the case that the results of this paper represent a small step towards the truth on the solvability of Diophantine equations of the type being considered. Not surprisingly, the *abc* conjecture shows that much stronger statements hold. In this section, we attempt to exhibit how far the above results are from the truth by describing a very strong Diophantine result under the hypothesis of the *abc* conjecture. For more on the *abc* conjecture and its consequences, the reader may wish to refer to the paper of Nitaj [14], that of Browkin [1], or that of Ribenboim [17].

The *abc* conjecture Given any $\epsilon > 0$, there exists $C = C(\epsilon) > 0$, depending only on ϵ, with the property that for all triples of positive integers a,b,c satisfying $(a,b,c)=1$ and $c=a+b$, the inequality

$$c < C \cdot N(a,b,c)^{1+\epsilon}$$

holds, where $N(a,b,c)$ denotes the product of distinct primes dividing abc.

Theorem 4.1 *Let a,b,c,d,e be nonzero integers. Then the abc conjecture implies that the equation*

$$(ax^m+b)(cy^n+d) = ez^2 \tag{4.1}$$

has only finitely many solutions (x,y,z,m,n) satisfying $xyz \neq 0$, $dax^m \neq bcy^n$ and $\min(m,n) \geq 5$.

In particular, the *abc* conjecture shows that there are only finitely many positive integers (x,y,z,m,n), with $z>0$, $x^m \neq y^n$, and $\min(m,n) \geq 5$, such that

$$(x^m-1)(y^n-1) = z^2. \tag{4.2}$$

If the exponent 2 in (4.1) is replaced by an integer $k > 2$, a much stronger statement can be derived from the *abc* conjecture. We will forego this endeavour, and content ourselves with Theorem 4.1.

It would be of interest to determine a heuristic argument which would indicate the Diophantine nature of the above problem in the case that $\min(m, n) < 5$. Even for the particular equation

$$(x^3 - 1)(y^3 - 1) = z^2, (x \neq y)$$

we do not have any reason to believe that there should be only finitely many integer solutions, nor do we have an argument which suggests that there are infinitely many integer solutions. Fritz Beukers has shown that for any nonsquare $d > 1$, the equation $-dz^2 = (x^3 - 1)(y^3 - 1)$ has infinitely many solutions (x, y, z).

References

[1] J. BROWKIN *The abc-Conjecture*, Number Theory, 75-105, Trends Math., Birkhäuser, Basel, 2000.

[2] R.D. CARMICHAEL *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$ Annals of Math. **15** no. 1-2 (1915), 30-70.

[3] J.H.E. COHN *Perfect Pell powers* Glasgow Math. J. **38** (1996), 19-20.

[4] J.H.E. COHN. *The Diophantine equation* $x^4 - Dy^2 = 1$ *II.* Acta Arith. **78** (1997), 401-403.

[5] P. CORVAJA AND U. ZANNIER *Diophantine equations with power sums and Universal Hilbert Sets*, Indag. Math. N.S. **9**, 317-332.

[6] H. DARMON AND L. MEREL *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81-100.

[7] C. FUCHS, R.F. TICHY *Perfect powers in linear recurring sequences*, preprint, 2001.

[8] L. HAJDU AND L. SZALAY *On the diophantine equations* $(2^n-1)(6^n-1) = x^2$ *and* $(a^n-1)(a^{kn}-1) = x^2$ *Period. Math. Hungar.* **40** (2000), 141-145.

[9] F. LUCA AND P.G. WALSH. *On the product of like-indexed terms in binary recurrence sequences.* To appear in the Journal of Number Theory.

[10] C. KO *On the diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$ Sci. Sinica **14** (1965), 457-460.

[11] D.H. LEHMER. *An extended theory of Lucas functions.* Ann. Math. **31** (1930), 419-448.

[12] W. LJUNGGREN *Some theorems on indeterminate equations of the form* $\frac{x^n-1}{x-1} = y^q$ (Norwegian) Norsk Mat. Tidsskr. **25** (1943), 17-20.

[13] F. LUCA *Multiply perfect numbers in Lucas sequences with odd parameters* Publ. Math. Debrecen **58** (2001), 121-155.

[14] A. NITAJ *La conjecture abc. (The abc conjecture)* Enseign. Math., II. Ser. 42 (1996), 3-24.

[15] A. PETHŐ *Diophantine properties of linear recursive sequences II.* preprint, 2001.

[16] P. RIBENBOIM *Catalan's Conjecture: Are* 8 *and* 9 *the only consecutive powers?* Academic Press, Boston, 1994.

[17] P. RIBENBOIM *ABC Candies*, J. Number Theory **81** (2000), 48-60.

[18] T.N. SHOREY, C.L. STEWART *Pure powers in recurrence sequences and some related diophantine equations* J. Number Theory **27** (1987), 324-352.

[19] L. SZALAY *On the diophantine equation* $(2^n - 1)(3^n - 1) = x^2$ Publ. Math. Debrecen **57** (2000), 1-9.

[20] P.G. WALSH *On Diophantine equations of the form* $(x^m - 1)(y^n - 1) = z^2$ Tatra Mt. Math. Publ. **20** (2000), 1-3.

F. Luca
Instituto de Matemáticas UNAM
Campus Morelia
Ap. Postal 61-3 (Xangari)
CP 58 089
Morelia, Michoacan
Mexico
fluca@matmor.unam.mx

P.G Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada
K1N-6N5
gwalsh@mathstat.uottawa.ca